ORACLE

# Oracle Database Security Assessment Tool FAQ

Protecting sensitive and regulated business data is mission critical. However, most organizations struggle to ensure their databases are securely configured, to understand who has access, and to know where sensitive data resides. Oracle Database Security Assessment Tool (DBSAT) helps identify potential risks in your database configuration, operation, or implementation and recommends changes and controls to strengthen your security.

## General

**What are the primary use cases for Oracle Database Security Assessment Tool (DBSAT)?**

DBSAT helps you assess database security, track user access and entitlements, and identify where sensitive data resides. It also supports your compliance and regulatory needs.

**How does DBSAT work?**

DBSAT includes three components: collector gathers data; reporter analyzes it and creates a Security Assessment report; discoverer finds sensitive data and generates a detailed Sensitive Data Assessment report.

**What type of data is collected and analyzed?**

DBSAT reviews database accounts, roles, auditing, data encryption, access controls, configuration, and related operating system settings—giving you a clear security overview at a glance.

The discoverer locates sensitive data by scanning column names and comments, and then groups results by categories like identification, financial, health, or academic information.

The sensitive data categories can be customized to meet different requirements.

**What is the performance impact of running DBSAT?**

DBSAT minimizes performance impact by reading only configuration files and data dictionary views. It never accesses your application data.

**How much time is required to learn how to run DBSAT and analyze the data?**

DBSAT is easy to learn. You can go from installation to complete reports in as little as 10 minutes. For large databases with thousands of users and role grants, analysis may take longer.

**Can I run DBSAT on my databases that are deployed in the Cloud?**

DBSAT can be used whether your database runs on-premises, in Autonomous AI Databases (Serverless, Dedicated, or Cloud@Customer), Database@Azure, Database@AWS, Database@GCP, customer-managed Database Cloud Services, BaseDB, or IaaS-deployed databases. Other prerequisites apply. Please refer to the documentation. To automate assessments and manage security at scale, consider using Oracle Data Safe or Audit Vault and Database Firewall.

**Can I run it on Autonomous AI Databases?**

Yes. DBSAT is certified for Autonomous AI Lakehouse, Autonomous AI Transaction Processing (ATP), and Autonomous AI JSON Database in serverless, dedicated, or Cloud@Customer deployment models.

**Will DBSAT provide me with different recommendations depending on the database type?**

Yes. DBSAT identifies the target type and performs specific checks on whether your databases run on-premises or in-cloud. DBSAT differentiates between on-premises databases, Autonomous AI Database, and Base Database Service. DBSAT provides specific recommendations for each of the database types.


Copyright © 2026, Oracle and/or its affiliates / Public

ORACLE

# DBSAT collector and reporter

### How do I run the DBSAT collector?

To run DBSAT collector:

```
$ dbsat collect <username>@<service_name> <dest-file>
```

- <username>@<service_name> is the connection string for the target database.
- dest-file is the name of the output file created by the collector, without the extension suffix.

Example command (*nix):

```
$ dbsat collect dbsat_user@pdb1 pdb_assessment
```

Example command (Windows):

```
C:\>dbsat.bat collect "dbsat_user@pdb1" pdb_assessment
```

As the DBSAT collector analyzes both database and operating system configuration, it is recommended that you run the DBSAT collector from the same host where the database server is running. If you cannot run it locally, you can run DBSAT collector remotely.

To get the reports, you need to run the DBSAT reporter (described below).

### How do I run the DBSAT reporter?

The run DBSAT reporter:

```
$ dbsat report <dest-file>
```

The `dest-file` is the JSON or DBSAT output file name produced by the collector, excluding the file extension. The same pathname is used as the base for all report files created by the DBSAT reporter, with appropriate suffixes added for the Text, HTML, JSON, and XLS report formats. For example,

```
$ dbsat report pdb_assessment
```

As DBSAT report output is encrypted by default and you will need to extract its contents:

```
$ dbsat extract pdb_assessment_report
```

After extracting the encrypted files, you will see the report with all the findings in multiple formats (HTML, XLSX, JSON, and TEXT).

### What is a finding?

The Database Security Assessment report presents findings to help improve your security posture.

Each finding include:

1. **Rule ID**: The Rule ID has two parts: the prefix identifies the report section, and the suffix identifies the specific rule.
2. **One-line summary**: One-line summary highlighting the objective and context of each check.
3. **Status**: The Status helps you prioritize implementing DBSAT recommendations. It indicates the level of risk associated with the finding, allowing you to make informed decisions about remediation.
4. **Summary**: Provides a summary of the Finding. When the Finding is informational, the summary typically reports only the number of examined data elements.
5. **Details**: Provides detailed information to explain the finding summary, typically results from the assessed database, followed by any recommendations for changes.
6. **Remarks**: Explain the reason for the rule and recommended actions for remediation.
7. **References**: Lists any relevant standards or guidelines associated with the finding, such as an Oracle Recommended Practice (ORP) related to an Oracle Database 19c STIG V1R1, Oracle Database 19c CIS Benchmark v1.2 recommendation, or related to a GDPR Article/Recitals.
8. **Documentation**: When the assessed Oracle Database is version 19c or 26ai, DBSAT will display documentation links relevant to each finding's remarks.


Copyright © 2026, Oracle and/or its affiliates / Public

### Can I extract certain Findings, compare different reports, or create an aggregated report for multiple databases?

DBSAT reporter and discoverer provide reports in JSON format to make further processing of the results possible.

Alternatively, for enterprise-wide, automated, and continuous security assessments, consider Oracle Data Safe or Oracle Audit Vault and Database Firewall. These solutions extend beyond DBSAT by enabling scheduled assessments, centralized reporting, historical tracking, and advanced compliance features. Details on these products and DBSAT appear later in this document.

### Can I run DBSAT collector on a multitenant pluggable database?

Yes. However, DBSAT must be executed for the root container and each PDB individually. DBSAT includes CDB-specific checks.

### Can I add my custom security assessment rules?

Custom assessment rules aren't supported. DBSAT is designed for quick setup, built-in best practices, and out-of-the-box compliance so you get immediate value with minimal setup. If you would like to add a new check to DBSAT, we encourage you to submit an Enhancement Request through My Oracle Support - each request is carefully reviewed for potential inclusion in future releases. Additionally, DBSAT supports the creation and customization of sensitive data discovery rules. You can add or customize sensitive type patterns and categories to meet your specific data discovery needs.

## DBSAT discoverer

### How does DBSAT discoverer work?

DBSAT discoverer uses a configuration file, one or more pattern files describing sensitive data types, and regular expressions to search column names and column comments. DBSAT discoverer does not query the data, only the metadata associated with the column names and column comments.

e.g., To search for “First Name”, you could use:

```
[FIRST NAME]
COL_NAME_PATTERN = (^|[_-])(FNAME|(FIRST|GIVEN).*(NAME|NM)|FORE.?(NAME|NM))($|[_-])
COL_COMMENT_PATTERN = (FIRST|GIVEN) NAME|FORENAME
SENSITIVE_CATEGORY = Identification Info - Public IDs
```

DBSAT comes with the initial configuration and pattern file, but customers can add custom sensitive types and categories or subcategories.

For a more thorough approach to identifying sensitive data, you might want to check out Oracle Data Safe Sensitive Data Discovery. In addition to analyzing column names and comments, Data Safe also scans the data itself, allowing it to identify sensitive information more accurately.

### What types of regular expressions are used?

DBSAT discoverer supports Extended Regular Expressions (ERE). This syntax is standardized by IEEE and is commonly used in Java.

For example, `(^JOB.*(TITLE|PROFILE|POSITION)$)|^POSITION` matches a string that starts with JOB (^JOB), followed by zero or more occurrences (*) of any character (.), and ends in ($) TITLE or PROFILE or POSITION. Or (|), it matches a string that starts (^) with POSITION.

### How accurate are the pattern-matching rules? How does one deal with false positives?

The rules provided with DBSAT were created to reduce false positives. However, as DBSAT examines only the column names and column comments, it might generate false positives. One way to reduce false positives is to edit the pattern file and tune the regular expression for your specific data model; another is to exclude schemas, tables, and columns from the search using an exclusion list file. As the CSV report includes a fully qualified name for the column (Schema.Table.Column), you easily exclude false positives by copying and pasting from the CSV report to the exclusion list file.

### Can DBSAT find sensitive data if my data model is in other languages besides English?

Along with a pattern file that searches English-based column names and comments, DBSAT also includes additional sample pattern files for Dutch, French, German, Greek, Italian, Portuguese, and Spanish that can help you quickly get started to discover sensitive data in non-English-based data models. Also, you can create your own pattern files from scratch or copy an existing one and adapt it to your requirements.

### How do I run the DBSAT discoverer?


Copyright © 2026, Oracle and/or its affiliates / Public

To run DBSAT discoverer:

```
$ dbsat discover -c <config file> <dest-file>
```

Example command (*nix):

```
$ dbsat discover -c Discoverer/conf/dbsat.config dbdata
```

**Do I need to run the DBSAT collector before running DBSAT discoverer?**

No. DBSAT discoverer is a standalone component. There is no dependency on the DBSAT collector or the reporter. You can choose to run it or skip it.

## Security Considerations

**What privileges are required for the user account connecting to the database to collect data?**

While a database user account with the Oracle-provided DBA role has the necessary privileges, you should follow the principle of least privilege. Please refer to the documentation for the minimum privileges needed to run DBSAT. In addition, the operating system user running DBSAT collector must have permission to read the ORACLE_HOME and TNS_ADMIN directories and files.

**How does DBSAT protect the collected configuration data and generated reports?**

By default, DBSAT output files are encrypted. We strongly recommend always keeping output files encrypted to ensure the security and confidentiality of your database assessment results. To decrypt the output files, you can use the `dbsat extract` command.

**What are the security risks of running DBSAT on production databases?**

The security risk of running DBSAT on production databases is minimal. DBSAT only reads configuration and metadata. All database actions performed by DBSAT are read-only and you can even run it on a read-only Data Guard standby database.

DBSAT should always be executed with the least privileges required to gather the necessary data for analysis. To ensure transparency and control, customers can run common diagnostic tools to validate what operations DBSAT executes during collection process. You can also examine the DBSAT collector output (in JSON format) to see what data was collected. Access to DBSAT-generated reports should be restricted, and the user account created for running DBSAT should be promptly dropped or locked once the assessment is complete.

## Download and Installation

**Where can I download the Oracle DBSAT?**

DBSAT can be downloaded from My Oracle Support under KB101686.

**How do I install DBSAT?**

DBSAT is provided as a zip file. Unzip it to install.

```
$ unzip dbsat.zip -d <directory>
```

**Which database versions are supported?**

DBSAT supports Oracle Database 11.2.0.4 and later releases, up to version 26ai.

**Which platforms are supported?**

DBSAT is supported on:

- Linux x86-64 and Linux 64-bit ARM
- Windows x64

For the following platforms, you must run the collector without encrypting the output by using the `-n` flag:

- Oracle Solaris on x86–64 (64-Bit)
- HP-UX Itanium (64-Bit)

DBSAT runs on most supported Oracle Database platforms. However, the DBSAT collector does not currently collect OS data from database servers running on the Windows platforms or if executed remotely. In Unix/Linux systems, it must


Copyright © 2026, Oracle and/or its affiliates / Public

execute under the BASH shell. If the BASH shell is unavailable, install it or execute the collector remotely from a server with it.

### Can Oracle download DBSAT and run it for me?

Oracle Solution Engineers or Oracle Consulting can help you run a database security assessment, analyze your results, and prioritize the next steps for your organization. Contact your sales team to get started.

## Product Licensing and Support

### How is DBSAT distributed?

DBSAT is available at no extra cost to all Oracle customers with an active Oracle Support contract.

### How can I report bugs or request enhancements for DBSAT?

Submit a service request for DBSAT via the My Oracle Support portal.

### Where do I go to get the bug fixes for DBSAT?

There are no independent patches or updates for DBSAT. Before running DBSAT, check My Oracle Support and download the latest version.

## DBSAT and Data Safe

### How does DBSAT relate to Data Safe?

Data Safe is a database security cloud service that provides a comprehensive suite of security capabilities. These capabilities include Security Assessment, User Assessment, Activity Auditing, SQL Firewall, Sensitive Data Discovery, and Data Masking and work for databases running in-cloud or on-premises.

DBSAT is excellent for assessing the current security state of a few databases. Data Safe addresses enterprise-level requirements. With Data Safe, you'll be able to:

- Schedule and execute recurring assessments
- Establish and manage database security baselines
- Compare security assessments and identify drift from baselines
- Receive real-time alerts on security findings
- Review the full history of assessment runs
- Gain insights into user risks through User Assessment
- Meet regulatory requirements by anonymizing non-production data, monitoring database activity, assessing security posture, and discovering sensitive data, all in a unified console
- Automate and integrate Data Safe capabilities into existing processes using APIs

To learn more about Oracle Data Safe, please visit oracle.com/security/database-security/data-safe/.

## DBSAT and Audit Vault and Database Firewall

### How does DBSAT relate to Audit Vault and Database Firewall?

Oracle Audit Vault and Database Firewall (AVDF) is a software appliance you can deploy on-premises or Oracle Cloud Infrastructure using a marketplace image. AVDF 20.9 introduced Database Security Posture Management, and it now provides a centralized security assessment solution for enterprises by integrating the popular Database Security Assessment Tool for Oracle Databases. The full-featured assessment with compliance mappings and recommendations helps organizations understand their security posture for all their Oracle Databases in one central place. With Audit Vault and Database Firewall, you'll be able to:

- Set a database security baseline
- See a comparison report with the drift against the baseline
- Get insight into user entitlements
- Address your company or regulatory requirements requiring database activity monitoring, assessing your database security posture, and preventing SQL injection attacks.


Copyright © 2026, Oracle and/or its affiliates / Public

To learn more about Oracle Audit Vault and Database Firewall, please visit oracle.com/security/database-security/audit-vault-database-firewall/.

## More Information

**Where can I find more information on DBSAT?**

Learn more at oracle.com/security/database-security/assessment-tool.

**Where do I go for more details on the Oracle Database Security Assessment program?**

Multiple Oracle teams across the globe have created their Oracle Database Security Assessment programs. Please talk to your Oracle Account Manager for assistance.


Copyright © 2026, Oracle and/or its affiliates / Public

## Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle

Copyright © 2026, Oracle and/or its affiliates. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.